19 August 2016 Study · Digital Identity · Web & Cloud

Flexible Two-Factor Authentication with FIDO

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/flexible-two-factor-authentication-with-fido/

FIDO Universal Second Factor (U2F) is an industry standard for a generally applicable two-factor authentication. Using a USB security token users can authenticate against a variety of web services. A key feature of the U2F concept is that the corresponding hardware element is physically connected at the time of registration process with the computer, so that the web browser can interact directly via a suitable interface. The wide applicability of FIDO U2F precludes that certified hardware element is required. This impedes, for example, the applicability of U2F applications on smart phones, since it is often not feasible to connect USB tokens to these devices. Often, due to lack of support, NFC is also no viable alternative.

In the course of this project, a solution was sought to allow the U2F registration process also in those situations when the availability of software or hardware is not given. Building on the existing architecture of a central key storage solution CrySIL, available as open source software, a concept was developed to offer FIDO for any platform. The suitability of the propagated solution was demonstrated during deployment. Specifically, an extension has been implemented for the Firefox Web browser, which complements the natively not given FIDO support and enables communication with an emulated U2F token, realized on the side of CrySIL.

Links

[CrySIL Sourcecode Repository

](https://github.com/IAIK/CrySIL)